PayPal™

Payflow Pro – HTTPS Interface Developer's Guide

For Professional Use Only
Currently only available in English.

A usage Professional Uniquement
Disponible en Anglais uniquement pour l'instant.

Last updated: May 2009

Payflow Pro – HTTPS Interface Developer's Guide

Document Number: 200038.en_US-200905

© 2009 PayPal, Inc. All rights reserved. PayPal is a registered trademark of PayPal, Inc. The PayPal logo is a trademark of PayPal, Inc. Other trademarks and brands are the property of their respective owners.
The information in this document belongs to PayPal, Inc. It may not be used, reproduced or disclosed without the written approval of PayPal, Inc.
Copyright © PayPal. All rights reserved. PayPal (Europe) S.à r.l. et Cie., S.C.A., Société en Commandite par Actions. Registered office: 22-24 Boulevard Royal, L-2449, Luxembourg, R.C.S. Luxembourg B 118 349.
Consumer advisory: The PayPal™ payment service is regarded as a stored value facility under Singapore law. As such, it does not require the approval of the Monetary Authority of Singapore. You are advised to read the terms and conditions carefully.

Notice of non-liability:
PayPal, Inc. is providing the information in this document to you "AS-IS" with all faults. PayPal, Inc. makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein. PayPal, Inc. assumes no liability for damages (whether direct or indirect), caused by errors or omissions, or resulting from the use of this document or the information contained in this document or resulting from the application or use of the product or service described herein. PayPal, Inc. reserves the right to make changes to any information herein without further notice.

Contents

Contents

Preface

This Document

This document describes the HTTPS interface, which allows you to post transactions directly to the Payflow servers. Use the HTTPS interface for all operating systems and language besides Java and .NET.

Revision History

Date	Description
April 2009	Minor updates for technical accuracy.
February 2008	Updated test and live URLs.
December 2007	Clarification that the related SDKs referred to in this guide are Payflow, not PayPal, SDKs. Update of test and live URLs. Remove Client Certification ID header. Reference to Developer's Guide for more information on transaction result values.
August 2007	First version of this document.

1 About the HTTPS Interface

This chapter contains the following topics:

Overview

The HTTPS interface allows you to post transactions directly to the Payflow servers.

NOTE: If you are programming in Java or .NET, you can simplify the implementation by using a Payflow SDK. The Payflow SDKs are based upon this HTTPS interface. Payflow SDK, Version 4 or later for .NET, can be used with classic ASP. For information on the Payflow SDKs, go to Developer Central at the URL below and click the **SDK and Downloads** link on the **Library** tab.

http://www.paypal.com/developer

This guide contains the information you will need to construct the HTTPS message. The body of the transaction is in name-value pair (NVP) or XMLPay format. For details on the NVP format, see the appropriate guide:

- *Payflow Pro Developer's Guide*
- *Website Payments Pro Payflow Edition Developer's' Guide*

For details on XMLPay format, see the appropriate XMLPay guide:

- *Payflow Pro XMLPay Developer's Guide*
- *Website Payments Pro Payflow Edition - XMLPay Developer's' Guide*

Moving From the Payflow SDK to the HTTPS Interface

The Payflow SDK, Version 3 or earlier, contains APIs that do the following:

1. Create a connection with the Payflow server
2. Submit the transaction
3. Destroy the transaction

When you move to the HTTPS interface, you will have to rewrite these portions of the code. You will need to complete four steps:

1. Write code that creates an HTTPS connection with the Payflow server.
2. Write an HTTPS request to submit your transaction data.
3. Receive the HTTPS reponse and extract the parameters.
4. Add code for error handling, retry logic, and duplicate transaction handling.

Getting Sample Code

For sample code, visit the Payflow Gateway forum in the PayPal Developer Community.

Contacting Support

For support, post your question or issue on the Payflow Gateway forum or open a ticket on the Contact Support tab at https://www.paypal.com/mts.

2 Reference

This chapter contains the following topics:

URLs for Sending Messages

Use the following URLs for sending transactions to PayPal's Payflow servers:

- Production (Live): `https://payflowpro.paypal.com`
- Pilot (Test): `https://pilot-payflowpro.paypal.com`

HTTPS Headers

Standard HTTPS Headers

HTTPS Header	Description	Req?
`Connect`	State of the connection. The server returns the value `close` to close the connection after the response is sent.	No
`Content-Length`	Size of message body.	Yes
`Content-Type`	Provide one of the following values: • `text/namevalue`: transaction request body is in NVP format. • `text/xml`: transaction request body is in XMLPay 2.0 format.	Yes
`Host`	Provide one of the two host URLs: • Production: `payflowpro.paypal.com` • Pilot (test): `pilot-payflowpro.paypal.com`	Yes

PayPal Protocol Headers

Protocol Header	Description	Req?
X-VPS-REQUEST-ID	A unique identifier for each request, whether the request is a single NVP transaction or an XMLPay 2.0 document with multiple transactions. This identifier is associated with all the transactions in a particular request. You must provide the X-VPS-REQUEST-ID value in the transaction request. The Payflow server uses the X-VPS-REQUEST-ID to check for duplicate transaction requests. When a transaction request is received, the server checks to see if the X-VPS-REQUEST-ID has been used before by this merchant. • If the X-VPS-REQUEST-ID has been used before, the server views it as a retry transaction, and the transaction is treated as a duplicate. The response to the original transaction is returned to the merchant, but a name-value pair of DUPLICATE=1 is added to indicate that this transaction is a duplicate. **IMPORTANT:** If you send new transaction data with a previously used X-VPS-REQUEST-ID, the server ignores the new data and returns the response to the original transaction associated with that X-VPS-REQUEST-ID. In Manager, duplicate transactions are associated with the TENDERTYPE N. It is very important that you check transaction responses for DUPLICATE=1. If the transaction is not a retry of an original failed transaction request, you must change the Request ID. • If the X-VPS-REQUEST-ID has not been used before, the server stores the X-VPS-REQUEST-ID to ensure that the X-VPS-REQUEST-ID is not reused and then runs the associated transactions. Duplicate checking is designed for short-term retries (a few minutes to a few hours after the original transaction). Although the X-VPS-REQUEST-ID is stored for a minimum of 7 days, it is not recommended that you send a retry so long after the original transaction. Data type: 1 to 32 printable characters	Yes
X-VPS-CLIENT-TIMEOUT	Time-out value in seconds. A transaction times out if the elapsed time between ending the original transaction request and receiving the transaction response exceeds the value of X-VPS-CLIENT-TIMEOUT. The recommended value is 45.	Yes

Integrator-Provided Headers

These headers are extensions to the Payflow HTTPS interface. The extension parameters describe the version of the application and the application's environment.

NOTE: Even though these parameters are not required, it is strongly recommended that you send them.

Parameter	Description	Req?
X-VPS-VIT-INTEGRATION-PRODUCT	Identifies the product that is integrated with the Payflow server. Data type: string Examples: iPayment, ColdFusion, MIVA, shopping cart Default: blank	No
X-VPS-VIT-INTEGRATION-VERSION	Version of the software as defined by the integrator or vendor. Limited to the major version and one digit of the minor version. Data type: alphanumeric string in the format: <Major Version>.<Minor Version> Examples: 1.1, 4.5, 10.0, Linux2.1 Default: blank	No
X-VPS-VIT-OS-NAME	Name of operating system that the application is running on. Data type: string Examples: Linux, SunOS, Windows 2000, Windows NT, Windows XP, Mac OS X, Free BSD. Default: blank	No
X-VPS-VIT-OS-VERSION	Version of operating system that application is running on. Data type: string in the format XXX.X Example: 2.4 Default: blank	No
X-VPS-VIT-RUNTIME-VERSION	Version of runtime environment of the language that the application is running on. Data type: string in the format XXX.X Examples: 10.1, 2.5 Default: blank	No

Transaction Message

The transaction message communicates the initial transaction data to the server. It is made up of the transaction request and response.

NOTE: The examples below are in NVP format. XMLPay uses the same format as NVP except that the `content-type` is `text/xml` and the body of both the request and response contain the XML document.

Transaction Request

The transaction request consists of a transaction request header and body.

Transaction Request Header

The following is an example of a transaction request header associated with a message in NVP format:

```
Connect: close
Content-Length: ...
Content-Type: text/namevalue
Host: payflowpro.paypal.com
X-VPS-REQUEST-ID: 9a5534f7e4f3a5e5138b062e000b279a
X-VPS-CLIENT-TIMEOUT: 45
X-VPS-VIT-CLIENT-CERTIFICATION-ID: 33baf5893fc2123d8b191d2d011b7fdc
X-VPS-VIT-Integration-Product: MyApplication
X-VPS-VIT-Integration-Version: 0.01
```

Transaction Request Body

The transaction request body contains the transaction information. The following is an example of a transaction request body in NVP format:

```
TRXTYPE[1]=S&ACCT[16]=5105105105105100&EXPDATE[4]=0109&
TENDER[1]=C&INVNUM[8]=INV12345&AMT[5]=25.12&PONUM[7]=PO12345&
STREET[23]=123 Main St.&ZIP[5]=12345&USER[6]=jsmith&
VENDOR[6]=jsmith&PARTNER[8]=PayPal&PWD[8]=testing1
```

The bracketed numbers are length tags that allow you to use the special characters `&` and = in the value sent. See the *Payflow Pro Developer's Guide* for more information.

Transaction Response

The transaction response consists of a transaction response header and body.

Transaction Response Header

The following is an example of a transaction response header associated with a message in NVP format:

```
Connect: close
Server: VPS-3.033.00
X-VPS-REQUEST-ID: 9a5534f7e4f3a5e5138b062e000b279a
Date: Mon, 16 May 2005 22:48:06 GMT
Content-Type: text/namevalue
Content-Length: 145
```

`X-VPS-REQUEST-ID` is the same ID sent in the transaction request.

Transaction Response Body

The transaction response body contains the response to the request. The following is an example response body in NVP format:

```
RESULT=0&PNREF=V53A0A30B542&RESPMSG=Approved&AUTHCODE=882PNI&
AVSADDR=X&AVSZIP=X&IAVS=X&PREFPSMSG=No Rules Triggered&
POSTFPSMSG=No Rules Triggered
```

Common Problems

Problem	Description
Result value 1	User authentication error. Can be caused by: • Invalid login information or IP restrictions on the account. Verify that there are no IP restrictions in PayPal Manager. • Verify `USER`, `VENDOR`, `PARTNER`, and `PASSWORD`. Remember that `USER` and `VENDOR` are both the merchant login ID unless a Payflow `USER` was created. All field values are case-sensitive. • Not appending `/transaction` to the host URL. This requirement will be removed in the future.
Result value 26	Verify `USER`, `VENDOR`, `PARTNER`, and `PASSWORD`. Remember that `USER` and `VENDOR` are both the merchant login ID unless a Payflow `a` was created. All field values are case-sensitive.
No response received	Usually caused by posting to an incorrect host URL.

NOTE: For additional information on transaction result values, see the appropriate developer's guide: *Payflow Pro Developer's Guide* or *Website Payments Pro Payflow Edition Developer's Guide*.